WHAT IS CLAIMED IS:

1. A method for cryptographing information, which is executed in a server connectable to a terminal of a client through a network, the method comprising the steps of:

a) generating a private encryption key and a public key for information encryption;

b) sending the generated public key and an encryption execution module to the client terminal;

c) executing the encryption execution module and the public key in the client terminal to encrypt the information and receiving the encrypted information from the client terminal; and

d) calling the generated private encryption key and decrypting the received encrypted information with the called private encryption key.

2. The method as set forth in claim 1, wherein the encrypted information is user authentication information required to log in and wherein the method further comprising the steps of:

e) comparing the decrypted information with prestored information; and

f) allowing or denying access of the client according to a result of information authentication

3. The method as set forth in claim 1, wherein the encrypted information is payment information and wherein the method further comprising the steps of:

e) sending the decrypted information to a connectable financial payment institution server; and

f) receiving payment approval result information from the financial payment institution server and sending to the client terminal the received payment approval result information;

4. The method as set forth in any one of claims 1 to 3, wherein the public key is generated by calculating coordinates of a point on an elliptic curve with a private encryption key value of n bits and an elliptic curve initialization value.

5. The method as set forth in any one of claims 1 to 3, wherein the step d) includes the steps of:

d-1) decrypting an encryption compression key contained in the encrypted information with the called private encryption key;

d-2) decompressing an original message and a digest message with the decrypted encryption compression key;

d-3) digesting the decompressed original message; and

d-4) comparing the digested original message with the

digest message and, if the digested original message and the digest are the same, decrypting the decompressed original message with the private encryption key.

6. A method for cryptographing information, which is executed in a computer connectable to a gateway communicating with at least one wireless terminal, the method comprising the steps of:

a) generating a private encryption key and a public key for information encryption;

b) sending the generated public key and an encryption execution module to the wireless terminal;

c) executing the encryption execution module and the public key in the wireless terminal to encrypt the information and receiving the encrypted information from the wireless terminal through the gateway; and

d) calling the generated private encryption key and decrypting the received encrypted information with the called private encryption key.

7. The method as set forth in claim 6, wherein the step d) includes the steps of:

d-1) decrypting an encryption compression key contained in the encrypted information with the called private encryption key;

d-2) decompressing an original message and a digest message contained in the encrypted information with the decrypted encryption compression key;

d-3) digesting the decompressed original message; and

d-4) comparing the digested original message with the digest message and, if the digested original message and the digest message are the same, decrypting the decompressed original message with the private encryption key.

8. A method for cryptographing information, which is downloaded together with a public key from an encryption server through a network and executed in a wired/wireless terminal of a client, the method comprising the steps of:

a) encrypting the information entered from a client with the public key to generate an original message;

b) digesting the encrypted original message;

c) compressing the original message and the digested original message with an encryption compression key under the condition that the encryption compression key is generated by randomly extracting a part of the public key;

d) encrypting the encryption compression key with the public key having been used to encrypt the original message; and

e) converting the compressed original message, the compressed digested original message and the encrypted

encryption compression key into Web documents and sending the Web documents.